

An Enhanced Privacy Preserving Buyer-Seller Protocol for Anonymous Transaction

¹Vinu V Das, ²J. FazlurRahman

¹Faculty of Computer Science & Engineering, Pacific University, Udaipur, India

²Professor Emeritus & Head (R&D Centre), HKBK College of Engineering, Bangalore, India

Email: ¹vinuvdas@gmail.com, ²jfazu2003@yahoo.co.in

Abstract: Due to the rapid growth of the internet and e-commerce, more and more digital products and multimedia contents are sold and transmitted over the internet. However, it also poses threats to copyright protection and to customers' privacy. Digital watermarks are used for protecting the digital contents from unauthorized duplication and distribution over internet. This can be achieved by inserting a unique digital watermark into each copy of the content before it is sold by the content owner (seller) to a buyer. This paper proposes a new enhanced privacy preserving Buyer-Seller watermarking protocol for anonymous transaction. Apart from solving the generic problems, this novel method is also finding solutions to Anonymity, Unlinkability and Loyalty marketing problem.

I. INTRODUCTION

The wide use of the internet and the rapid development of information and communication technology have facilitated the proliferation of online purchases of digital and multimedia contents. In turn all types of multimedia contents can be easily stored, traded, distributed and replicated in digital form without a loss of quality. In this context digital copyright protection of multimedia information is a main cause that needs to be addressed. On the other hand, how to protect the rights and provide security for both the sellers and the buyer is another challenge.

The encryption and digital watermarking are recognized as promising technique for network security and copyright protection. The encryption is to prevent unauthorized access to a digital content. But the limitation is that once the content is decryption, it doesn't prevent illegal replication by an authorized user. Digital watermarking [1, 6] complimented with encryption technique is to provide copyright ownership by embedding the seller's and buyer's identity in the distributed content. This is to trace and identify the copyright violation.

A buyer-seller watermarking protocol is one that combines encryption, digital watermarking, and other techniques to ensure protection of rights and privileges of both the buyer and the seller in ecommerce. An efficient buyer-seller watermarking protocol is expected to solve the following existing issues, apart from any another suggested new problems.

1. *The piracy tracing problem:* once a pirated copy is found, the seller or arbitrator should be able to trace and identify the copyright violator.
2. *The customer's rights problem:* since the seller is entitled to the responsibility of generating and inserting digital watermarks, they are granted access to each copy of the watermark or watermarked digital content. A malicious

seller may replicate the digital content illegally to from the innocent buyer for any piracy.

3. *Unbinding problem:* it is possible for the seller to intentionally transplant the watermark embedded in the pirated copy into another copy of the higher priced digital content, provided both copies are sold to the same customer, to produce made-up piracy so that the seller can get compensated more.

4. *The anonymity problem:* the identity of a buyer and the purchase history should remain unexposed during transactions unless he is proven to be guilty.

5. *Conspiracy problem:* a malicious seller may collude with an untrustworthy third party to fabricate piracy to frame an innocent buyer; on the other hand, a malicious buyer may collude with an untrustworthy third party can found the tracing of piracy by removing the watermark from digital content.

6. *Dispute resolution problem:* The buyer's participation in the dispute resolution is against the general practice of law, since it is the seller's responsibility to prove the guilty of the buyer not in reverse.

7. *Loyalty marketing problem:* The buyer being anonymous, the seller cannot give discounts to regular buyers or apply other loyalty marketing techniques.

Accordingly, a buyer-seller watermarking protocol should provide the following security properties as the strategic design principle.

1. *Traceability:* a copyright violator should be able to be traced and identified.
2. *Non-framing:* nobody can accuse an honest buyer.
3. *Non-repudiation:* a guilty buyer cannot deny his responsibility for a copyright violation caused by him.
4. *Dispute resolution:* the copyright violator should be identified and adjudicated without him revealing his private information, e.g. private keys or watermark.
5. *Conspiracy resistance:* no colluded parties should be able to frame an innocent buyer or to confound the tracing by removing the watermark from the digital content.
6. *Anonymity:* a buyer's identity is undisclosed until he is judged to be guilty.
7. *Unlinkability:* nobody can determine whether the different watermarked contents are purchased by the same buyer or not.

II. RELATED WORK

In the past many buyer-sellers watermarking protocols have proposed and the literature is rich in the relevant area.

Qiao and Nahrstedt [13] first pointed out the customer's rights problem in the watermarking protocols for piracy tracing. However, their scheme is symmetric and doesn't guarantee the buyer's security. The first known asymmetric buyer-seller watermark protocol was introduced by Memon and Wong [5], and it was improved by Ju et al. [16]. Since the first introduction of the concept, several alternative design solutions have

been proposed. Except that the piracy tracing problem and the customer's rights problem are resolved in the early schemes, the existing solutions to the other problems are either impractical or incomplete, as depicted in Table 1 – a Comparison of some the existing buyer-seller watermarking protocols with our Protocol.

TABLE I COMPARISON OF PROTOCOLS

Problem solved	Memon& Wong	Ju et al.	Choi et al.	Goi et al.	Lei et al.	Shao	Ibrahim et al.	Ours
Piracy tracing	X	X	X	X	X	X	X	X
Customer's rights	X	X	X	X	X	X	X	X
Unbinding					X	X	X	X
Conspiracy				X				X
Dispute resolution		X			X	X	X	X
Anonymity/unlinkability								X
Loyalty								X

1. *The piracy tracing problem.* All of these protocols are able to resolve the piracy tracing problem, and provide a mechanism for the seller to trace and recover the identity of a guilty buyer.

2. *The customer's rights problem.* All these protocols can solve the customer's rights problem, since the protocols are designed asymmetric, i.e., the seller doesn't know the exact value of the buyer's watermark, neither does they know the final watermarked digital content that the buyer gets. Therefore, the accused buyer for an illegal replication or distribution cannot claim that the copy is originated from the seller.

3. *The unbinding problem.* Lei et al. [4] addressed the unbinding problem in Memon & Wong, [5], (Ju et al., [16], Goi et al. [2] has provided a mechanism to bind a specific transaction of a digital content to a specific buyer, such that a malicious seller cannot transplant the watermark embedded in a digital content to another higher-priced content. The similar design principle is applied in Shao, [14].

4. *The conspiracy problem.* Choi et al. [17] pointed out the conspiracy problem of Memon & Wong, [5], Ju et al., [16] where a malicious seller can collude with an untrustworthy third party to fabricate piracy to frame an innocent buyer. Goi et al. [2] found the conspiracy problem couldn't be solved through commutative cryptosystems of Choi et al., [17], and further point out that the schemes of Memon & Wong, [5], Ju et al., [16], Choi et al., [17] are vulnerable against conspiracy attacks, and show that the protocol's security shouldn't rely on any third party. According to our analysis, we conclude that the protocols of Lei et al., [4], Shao, [14], and Ibrahim et al., [3] cannot resist the conspiracy attack, where a malicious seller can collude with a third party, such that the seller can discover the buyer's watermark.

5. *The anonymity problem.* Memon and Wong's protocol [5] requires the seller to know the buyer's identity to carry out a transaction. Protocols of Ju et al., [16], Choi et al., [17] improve Memon & Wong, [5] by applying an anonymous key pair in each transaction. However, both protocols require the WCA

to know the buyer's identity, which means that the buyer's anonymity is not preserved against conspiracy attacks. In Goi et al., [2], the buyer is required to request a signature from the certification authority (CA) of the public key infrastructure (PKI) to generate a watermark. However, Goi et al., [2] cannot solve the anonymity problem efficiently, since before each transaction, the buyer has to contact the CA for a new signature. Lei et al., [4], Shao, [14] apply anonymous certificates, i.e., digital certificates without real identities of applicants.

Next section proposes a new enhanced privacy preserving Buyer-Seller watermarking protocol for anonymous transaction. Apart from solving the above stated problems, this novel method is also finding solutions to Anonymity, Unlinkability and Loyalty marketing problem.

III. PROPOSED SYSTEM

The proposed protocol addresses many issues found in its predecessor such as *Dispute resolution problem*, *Anonymity*, *unlinkability problem* and it also fixes the *Loyalty marketing problem* along with other problems. The proposed model based on any public key cryptosystem has four different roles as follows.

1. **S:** The seller or the sales point, from where the buyer purchases the digital content. The seller may be the original owner of the digital content, or an authorized reselling agent or dealer.
2. **B:** The buyer, who wants to purchase a digital content from the seller S.
3. **CA:** The Certification Authority is responsible for issuing Public-Secret key pair (P_s, S_s), Temporary Public-Private key pair (TP_s, TS_s), Buyer and Seller recognition number (BR_k and SR_k) and watermark for individual digital content ($W_{s, PID}$), and functions to generate Authentication Key and embedding watermark. They may appoint trusted Regional Watermark Certification Authorities (RWCA) to share and reduce its workload.

4. **ARB**: An arbiter, who adjudicates lawsuits against the infringement of copyright and intellectual property.

This section restricts itself to further discussion on security or implementation issues related to the public key cryptosystem by assuming that a public key infrastructure has been well deployed so that each party has its own public-private key pair as well as a digital signature certificate issued by CA. Also assume that every member in transaction has the access to the watermarking extraction and detection algorithm software in the CA website, which is required to verify the originality of the product purchased. Before elaborating further on the proposed protocol, the notations used in this model are defined below.

X	The Digital Content embedded with watermark
X_o	Original copy of the Digital Content without any watermark
W	Generated Watermark, which is to be embedded into the digital content
PID	Unique number given by the CA to identify a digital content, which will be published for anyone who is likely to take part in the transaction
BRk	Buyer Recognition key issued by the CA
SRk	Seller Recognition key issued by the CA
$\oplus$	Watermark information binary Insertion operators into the original copy of digital content.
(P_B, S_B)	A public-secret key pair, where P_B is buyer's (or B's) public key and S_B is B's secret key.
TP_B, TS_B	A Temporary public-secret key pair, where TP_B is buyer's (or B's) public key and TS_B is B's secret key.
$E_{pb}(M)$	The message M is encrypted using B's public key(using the private key algorithm)
$E_{sb}(M)$	The message M is encrypted using B's private key(using the private key algorithm)
$D_{ps}(C)$	The cipher text C is decrypted using S's public key(using the private key algorithm)
$D_{ss}(C)$	The cipher text C is decrypted using S's private key(using the private key algorithm)
$EP_K(M)$	The message M is encrypted using the private key K (using the private key algorithm)
$DP_K(M)$	The message M is decrypted using the private key K (using the private key algorithm)

By $X \oplus W$ means,

$$x_1 \oplus w_1, x_2 \oplus w_2, \dots, x_n \oplus w_n, x_{n+1} \oplus w_{n+1}, \dots, x_m \oplus w_m \}$$

A privacy homomorphism with respect to the binary operator $\oplus$ is applied to insert a watermark W to any original copy of the digital content X. For every a and b in the message block, $\oplus$ has the property that

$$E_{PK}(a \oplus b) = E_{PK}(a) \oplus E_{PK}(b)$$

where PK is the public encryption key. The buyer-seller watermarking protocol in this section has three sub-protocols: *Registration Protocols*, *Watermarking Protocol* and

Arbitration Protocol.

A. Registration Protocols

Figure 1 show the registration protocol where the buyer is able to generate Temporary Public-Secret key pairs, and Buyer Recognition key, BRk, for the anonymous transaction. The Temporary keys and BRk can be used for as many as transaction without generating the further, till the buyer observes for a change. On the other hand seller is able to generate required Public-Secret key pairs and Seller Recognition key, SRk. This SRk can be used as a unique Seller Recognition code for any number of products (PIDs) to be sold over internet.

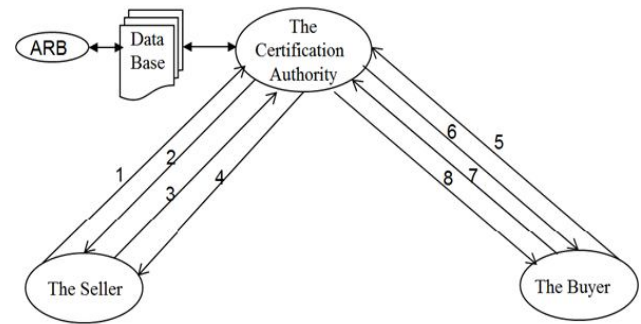


Figure 1 Registration protocol

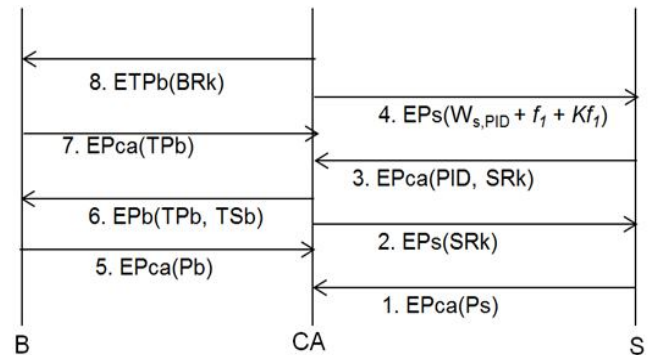


Figure 2 Transactions in the Registration protocol

Figure 2 visualizes the details of possible transactions in the proposed registration protocol. Step-by-step procedures of the transactions are given below:

1. S sends a request to CA for successfully registering with him to recognize him as the genuine seller.
2. CA responding to request by generating the Seller Recognition key, SRk.
3. S will have to register with CA for selling a product PID, EPca(PID, SRk).
4. CA will generate the watermark Ws and homomorphic function to embed the watermark with the digital content, X_o and a Key function to check the authenticity of the watermarked content.
5. B sends a request to CA to generate temporary Public-Secret key pairs to maintain the anonymity in the transaction.
6. CA responds by delivering the temporary key.(TPb, TSb)
7. Further to maintain increased anonymity in the

e-commerce, Buyer Recognition key, BRk, is requested.

8. CA issues BRk to B.

B. Watermarking Protocol

Figure 3 shows the transactions involved in the watermarking embedding protocol; where purchase order is placed once B is decided to purchase a product, PID, from S. To maintain anonymity, Buyer Recognition Key, BRk, and the product to be purchased, PID, along with the earlier received promotional coupon, PC, is forwarded.

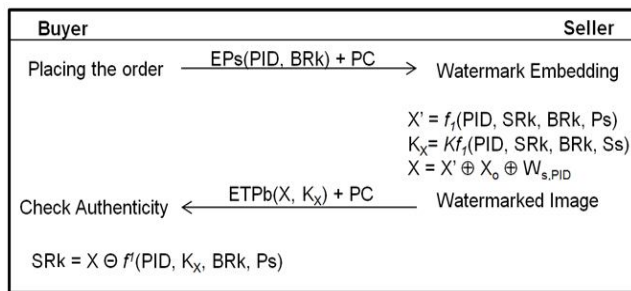


Figure 3 watermarking embedding protocol

If the any discount is applicable to PC forwarded, it is processed before the final invoice and payment confirmation is made. Watermark key, X^1 , is generated using the function f_1 from PID, SRk, BRk, and Ps. The authentication key, K_X , is generated using the key function Kf_1 with the help of PID, SRk, BRk, Ss. Now the watermark issued by the CA for the particular product, PID, for a seller, S, is embedded with the Watermark key, X^1 .

Watermarked digital content, X, along with the authentication key, K_X , and new promotional code is send to the S. The buyer, B, can check the authenticity (in the CA/RCA website by giving the PID and SRk) of the product purchased by checking the SRk which is extracted from the watermarked image X, using the homomorphic function $\ominus$ with the generated number from the function $f^1(\text{PID, } K_X, \text{BRk, Ps})$.

C. Arbitration Protocol

The identification and arbitration protocol is executed among the seller S, an Arbitrator ARB, and the CA,

In case S finds a pirated copy Y of X, she extracts the watermark $W_{s, \text{PID}}$ from Y, and searches sales record by correlating $W_{s, \text{PID}}$ and X' with the BRk of person (in the DB) who is possessing the digital content. If the required entry not found on the S's DB, it is further forward to the ARB for further inquiry and judgment.

The ARB, with the help of CA and X' , easily extracts the required information as the digital product, PID, is sold by whom to whom.

IV. CONCLUSION

In this paper, we presented different attacks on buyer-seller watermarking to prove that neither of these existing protocols is able to provide security for the buyer or the seller as claimed. We also address the anonymity, unlinkability and Loyalty problem in these protocols. We propose an improved

protocol, which is secure and fair for both the seller and the buyer. Our protocol employs privacy homomorphic cryptosystems and group signature schemes, in order to protect the secrecy of the buyer and the seller, and to preserve revocable anonymity of the buyer. Comparing with early work, our anonymous buyer-seller watermarking protocol is able to address all the required existing issues apart from anonymity, unlinkability and Loyalty problem.

REFERENCES

- [1] Cox, I., Miller, M., Bloom, J. & Miller, M. (2001), Digital Watermarking: Principles & Practice, The Morgan Kaufmann Series in Multimedia Information and Systems, Morgan Kaufmann.
- [2] Goi, B.-M., Phan, R. C.-W., Yang, Y., Bao, F., Deng, R. H. & Siddiqi, M. U. (2004), Cryptanalysis of two anonymous buyer-seller watermarking protocols and an improvement for true anonymity, in 'Applied Cryptography and Network Security', LNCS 2587, pp. 369-382.
- [3] Ibrahim, I. M., El-Din, S. H. N. & Hegazy, A. F. A. (2007), An effective and secure buyer-seller watermarking protocol, in 'Third International Symposium on Information Assurance and Security, 2007. IAS 2007', pp. 21-28.
- [4] Lei, C.-L., Yu, P.-L., Tsai, P.-L. & Chan, M.-H. (2004), 'An efficient and anonymous buyer-seller watermarking protocol', IEEE Transactions on Image Processing 13(12), 1618-1626.
- [5] Memon, N. D. & Wong, P. W. (2001), 'A buyer-seller watermarking protocol', IEEE Transactions on Image Processing 10(4), 643-649.
- [6] Hartung, F. & Kutter, M. (1999), Multimedia watermarking techniques, Vol. 87, pp. 1079-1107.
- [7] Vinu V Das and Nessay Thankachan, "A Buyer-Seller Watermarking Protocol for an Efficient and Secure Digital Transaction," in Proc. 1st Int. Conf. on Information System and Technology, India, 2007, pp. 127-132.
- [8] K Gopalakrishnan, N Memon, and PL Vora, "Protocols for Watermark Verification," IEEE Multimedia, Vol. 8, Oct-Dec 2001, pp. 66-70.
- [9] J Zhang, W Kou and K Fan, "Secure Buyer-Seller Watermarking Protocol," IEE Proc. Int. Conf. Security, Vol. 153, No. 1, March 2006.
- [10] Vinu V Das, "A Tree Based Buyer-Seller Watermarking Protocol," in Proc. 3rd Int. Joint Conf. on Computer, Information, Systems Sciences, and Engineering, USA, 2007.
- [11] Goi B-M, Phon R C-W, Yang Y, Bao F, Deng R H, and Siddiqi M U, "Cryptanalysis of two Anonymous Buyer-Seller Watermarking Protocols and an Improvement for true Anonymity," in Proc. Applied Cryptography and Network Security, 2004, LNCS 3089, pp. 369-382.
- [12] Cox, I., Kilian, J., Leighton, T. & Shamoon, T. (1997), 'Secure spread spectrum watermarking for multimedia', IEEE Transactions on Image Processing 6(12), 1673-1687.
- [13] Qiao, L. & Nahrstedt, K. (1998), 'Watermarking schemes and protocols for protecting rightful ownership and customer's rights', Journal of Visual Communication and Image Representation 9(3), 194 - 210.
- [14] Shao, M.-H. (2007), A privacy-preserving buyer-seller watermarking protocol with semitrust third party, in 'Trust, Privacy and Security in Digital Business', LNCS 4657, pp. 44-53.
- [15] Mina Deng and Bart Preneel (2010). Attacks on Two Buyer-

- Seller Watermarking Protocols and an Improvement for Revocable Anonymity, E-commerce, Kyeong Kang (Ed.), ISBN: 978-953-7619-98-5, InTech
- [16] Ju, H.-S., Kim, H.-J., Lee, D.-H. & Lim, J.-I. (2002), 'An anonymous buyer-seller watermarking protocol with anonymity control', Information Security and Cryptology – ICISC, pp. 421-432
- [17] JG Choi, K Sakurai, JH Park; "Does It Need Trusted Third Party? Design of Buyer-Seller Watermarking Protocol without Trusted Third Party", Applied Cryptography and Network Security, 2003 - Springer LNCS V 2846-